Security analysis of the XYZ protocol

Report for the Computer Security exam at the Politecnico di Torino

Giovanni Pautasso (31415)
tutor: Jack-The-Ripper

February 2011

Contents

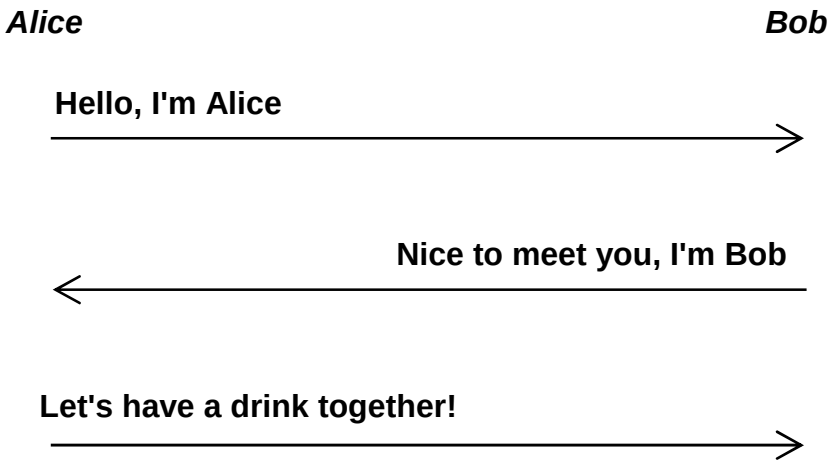

Figure 1: Handshake protocol.

1 Introduction

Explain here why the XYZ protocol is important and what was the purpose of the present work.

If you want to reference a web site you can do like this: http://www.polito.it.

2 Protocol description

Describe the protocol in detail, trying to demonstrate knowledge of the topics covered in the course. In other words, don't limit yourself just to list security features but explain why they are important and provide your opinion if they are correctly implemented or could be improved.

You can reference a figure by using the appropriate command, as in the case of Fig. 1, that will be automatically placed on the page and numbered by LaTeX.

You can also cite papers published at conferences, like [1], or journals [2] or an RFC [3].

If the section contains a lot of information, you may want to split it into different subsections, each one with a specific focus as done here.

2.1 Request format

The request contains the ID of the caller and the destination IP address, encoded in four different bytes.

2.2 Response format

The response contains a status code (three digits encoded in ASCII) followed by the answer encoded in ISO-8859-1 and terminate with CR LF.

data size (kB)	*raw transfer time* (ms)	*secure transfer time* (ms)
128	20	22
256	22	30
512	26	37
1024	30	99

Table 1: Experimental results.

3 Experimental evaluation

Describe:

- general purpose of the experiments (functional evaluation, performance evaluation, comparison with other stuff)
- experimental setup (hardware and software, including detailed build and configuration instructions if needed)

Then describe each experiment: its specific purpose (e.g. testing a specific feature of the protocol), the command run, and the output (expected and actual). You can use a table like Tab. 1 to group the results (for example if the same experiment was repeated with several data sizes)

For performance testing, remember to run not only experiments with various data size but also – in case of a client-server protocol – stress tests for the server (i.e. increasing number of clients simultaneously requesting attention from the server).

References

[1] P. Papadimitratos, G. Calandriello, J.-P. Hubaux, A. Lioy, "Impact of vehicular communication security on transportation safety", MOVE 2008: IEEE INFOCOM-2008 workshop on Mobile Networking for Vehicular Environments, Phoenix (AZ, USA), April 13-18, 2008, pp. 1-6

[2] W. Diffie, M.E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976, pp. 644–654

[3] R. Shirey, RFC-4949 "Internet Security Glossary, Version 2", August 2007